REMARKS/ARGUMENTS

Claims 1-7 and 10-19 were pending in this application before the present response. In the Office Action dated September 26, 2007, claims 1-7 and 10-15 stand rejected under 35 U.S.C. § 103, and claims 16-19 stand rejected under 35 U.S.C. § 102.

Claims 6, 11, and 16 are amended herein. No new matter is introduced by these amendments. The amendments to claims 6 and 11 correct typographical errors in the preamble.

No amendment made is related to the statutory requirements of patentability unless expressly stated herein. No amendment is made for the purpose of narrowing the scope of any claim. Any remarks made herein with respect to a given claim or amendment is intended only in the context of that specific claim or amendment, and should not be applied to other claims, amendments, or aspects of Applicants' invention.

Claims 1-7 and 10-19 are now pending in this application. Applicants respectfully request reconsideration and allowance of all pending claims, in view of the following remarks.

Claim Rejection – 35 U.S.C. § 102

Claims 16-19 stand rejected under 35 U.S.C. § 102(a) and 102(e) as being allegedly anticipated by Van Oorschot et al., U.S. Pat. No. 5,850,443 (hereinafter "Van Oorschot"). The Applicants respectfully traverse this rejection.

Anticipation requires that each and every element of the claims must be present in the cited reference. The Van Oorschot reference does not anticipate the claims, as amended.

The Van Oorschot reference describes a cryptographic key management system for mixed trust environments. The Van Oorschot system is a "hybrid system" because it involves both an asymmetric and a symmetric technique. The system uses a symmetric key to produce ciphertext data (*i.e.*, encrypted plaintext data). The system then uses an asymmetric technique to encrypt the symmetric key, and transfers the encrypted key with the ciphertext data to another party. The other party uses the asymmetric technique to decrypt the symmetric key, and uses the symmetric key to decrypt the ciphertext data. In contrast, independent claim 16, as amended, recites "wherein the cryptographic key, first key, and second key encrypt and decrypt data using a similar class of algorithm to encrypt and decrypt data". Since the Van Oorschot reference does not describe the use of a single cryptographic technique to encrypt and decrypt the keys, the Examiner should withdraw the 102 anticipation rejection as to independent claim 16.

Claims 17-19 depend from independent claim 16. For the previously stated reasons, independent claim 16 is allowable. Since any claim that depends from an allowable independent claim is also allowable, the Applicants respectfully submit that the Examiner should also withdraw this rejection as to dependent claims 17-19.

Claim Rejection – 35 U.S.C. § 103

Claims 1-7 and 10-15 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Menezes et al., Handbook of Applied Cryptography, 1997, section 13.3.1, pages 551-553 (hereinafter "Menezes"), in view of Weiant, Jr. et al., U.S. Pat. No. 6,044,350 (hereinafter "Weiant"). The Applicants respectfully traverse this rejection.

The difference between the claims, as amended, and the Menezes and Weiant references, taken either alone or in combination, are nonobvious. As reiterated by the Supreme Court in *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. __, 82 USPQ.2d 1385, 1391 (2007), the framework for the objective analysis for determining obviousness under 35 U.S.C. § 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Thus, the analysis of patentability under 35 U.S.C. § 103 requires consideration of four factors: (i) the scope and content of the prior art, (ii) the differences between the prior art and the claims as a whole, (iii) the level of ordinary skill in the art, and (iv) objective evidence of non-obviousness. *Graham* at 13. Combining elements from different prior art references in hindsight is to be avoided.

The Menezes reference describes a key layering technique for distributing cryptographic keys when confidentiality of the private and symmetric keys must be preserved. The layering technique consists of master keys at the highest level, key-encrypting keys, and data keys. The master keys are distributed manually or initially installed and protected by procedural controls or electronic isolation. The key-encrypting keys are used for transport or storage of other symmetric or encryption public keys. The data keys are used to provide cryptographic operations on user data, and may be either short-term symmetric keys or long-term asymmetric keys.

Since the layering technique described in the Menezes reference involves the use of both asymmetric and symmetric cryptographic techniques, the Menezes reference describes a "hybrid system". In contrast, independent claims 1 and 10 recite the limitations of a key hierarchy system and method that involves asymmetric cryptographic processing, not a hybrid system that involves symmetric and asymmetric processing.

Furthermore, the Menezes reference describes the key-encrypting keys as "symmetric or encryption public keys used for key transport or storage of other keys". In contrast, independent claims 1 and 10 recite the limitations of a key hierarchy system and method that describe "a second key for performing an asymmetric cryptographic processing operation to **update** the first key" (as recited in independent claim 1) and "**updating** the first asymmetrical cryptographically processed key from time-to-time" (as recited in independent claim 10).

The Examiner admits that the Menezes reference does not teach that the second key requires a second processing time greater than the first cryptographic processing time. To make up for this shortcoming, the Examiner relies on the Weiant reference.

The Weiant reference describes a system for a general-purpose computer that includes a digital certificate meter to certify an electronic commerce purchase by a user. For each purchase, the user interacts with the digital certificate meter to select a service rate that the system adds to the purchase to indemnify the purchase for a given amount. The user selects the service rate from a table of security and indemnification rates that the system displays to the user. In one embodiment, each row in the table includes a key identifier, length, security level, indemnification amount, service rate, and processing time. The user selects one of the rows from the table based primarily on the indemnification and service rate that is most appealing to the user. The system uses the private/public key pairs associated with the user's selection to encrypt the electronic commerce purchase.

The combination of the Menezes and Weiant references is not appropriate because a person of ordinary skill in the art would not look to the Weiant reference given the shortcomings of the Menezes reference. The Menezes reference describes a layering technique for distributing cryptographic keys in a hybrid key management system. The Examiner admits that the Menezes reference does not teach that the second key requires a second processing time greater than the first cryptographic processing time. To make up for this shortcoming, the person of ordinary skill in the art would look to other key hierarchy prior art, not to a prior art reference that describes a system for certifying an electronic commerce purchase by a user. In addition, the Menezes reference describes a hybrid system that uses both symmetric and asymmetric techniques. In contrast, the Weiant reference describes an electronic commerce digital certificate system that only uses an asymmetric encryption technique.

Furthermore, the Weiant reference only describes a general proposition that keys with different lengths have different processing times. Thus, the Menezes and Weiant references, taken either alone or in combination (assuming, arguendo, that one of ordinary skill in the art would be led to combine them), do not describe that "the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and that **requires** a second cryptographic processing time greater than the first cryptographic processing time" (as recited in independent claim 1) or that "the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity **requiring** a second amount of resources by the processing device that is higher than the first amount of resources" (as recited in independent claim 10).

For at least the aforementioned reasons, independent claims 1 and 10 are patentable over the Menezes and Weiant references, either taken alone or in combination. Thus, the Examiner should withdraw the 103 obviousness rejection as to independent claims 1 and 10.

Claims 2-7 and 11-15 depend, respectively, from independent claims 1 and 10. For the previously stated reasons, independent claims 1 and 10 are allowable. Since any claim that depends from an allowable independent claim is also allowable, the Applicants respectfully submit that the Examiner should also withdraw this rejection as to dependent claims 2-7 and 11-15.

For the rejection of claims 12-15, the Examiner takes Official Notice that "the resources include [processing time/transistor density on an IC/memory capacity/data bandwidth] because these resources are well-known tradeoffs of resource intensive actions as cryptography". The Applicants traverse the Examiner's assertion that these are well-known tradeoffs in the context of the claims. If the Examiner maintains the rejection of claims 12-15, the Applicants respectfully request, pursuant to MPEP 2144.03, that the Examiner produce documentary evidence that properly supports the assertion that these resources are well-known tradeoffs.

Conclusion

In view of the foregoing discussion, the Applicants believe that claims 1-7 and 10-19 are allowable over the cited art. The Applicants respectfully submit that all pending claims are in full condition for allowance, and earnestly request that the Examiner withdraw all objections and rejections of the claims and enter a Notice of Allowance at the earliest date possible.

Should the Examiner feel that there are any issues outstanding after consideration of this response, the Examiner is invited to contact Applicants' undersigned representative to expedite prosecution.

Respectfully submitted,
ERIC J. SPRUNK et al.

Date: January 25, 2008

BY: /Stewart M. Wiener/
Stewart M. Wiener
Registration No. 46,201
Attorney for Applicants

MOTOROLA, INC.
101 Tournament Drive
Horsham, PA 19044
Telephone: (215) 323-1811
Fax: (215) 323-1300